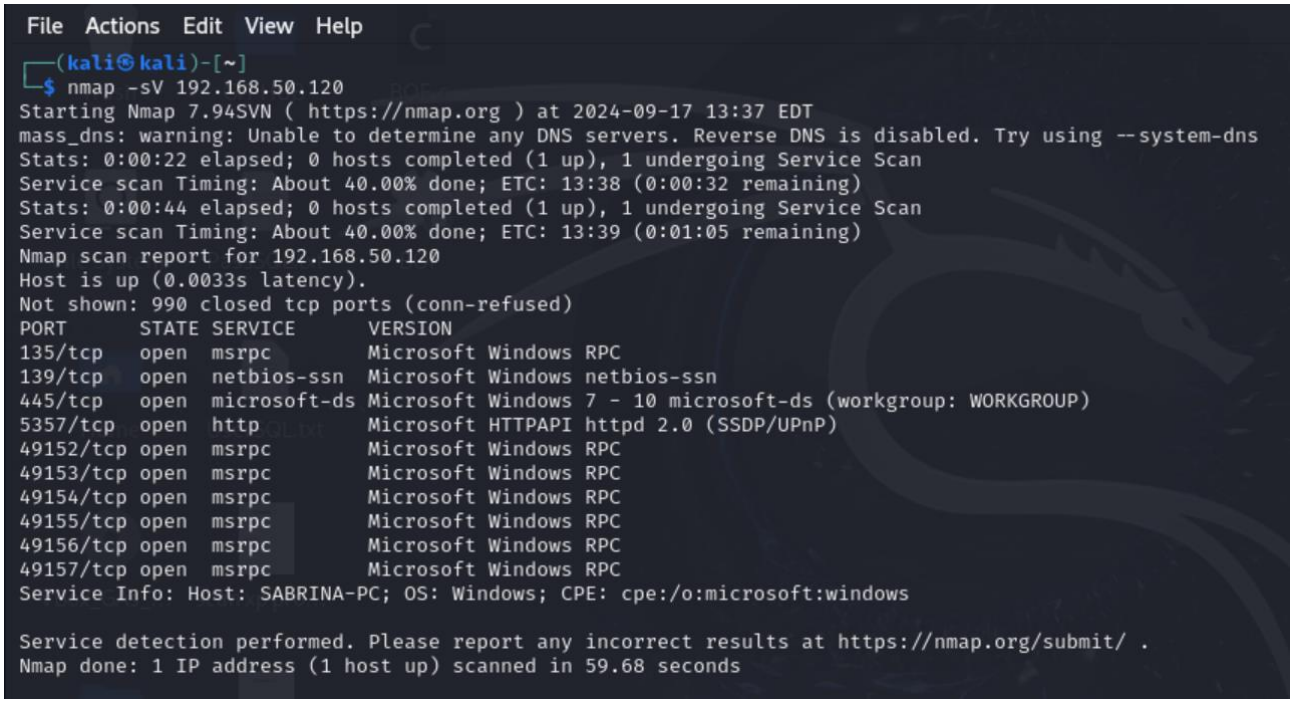
W18D1

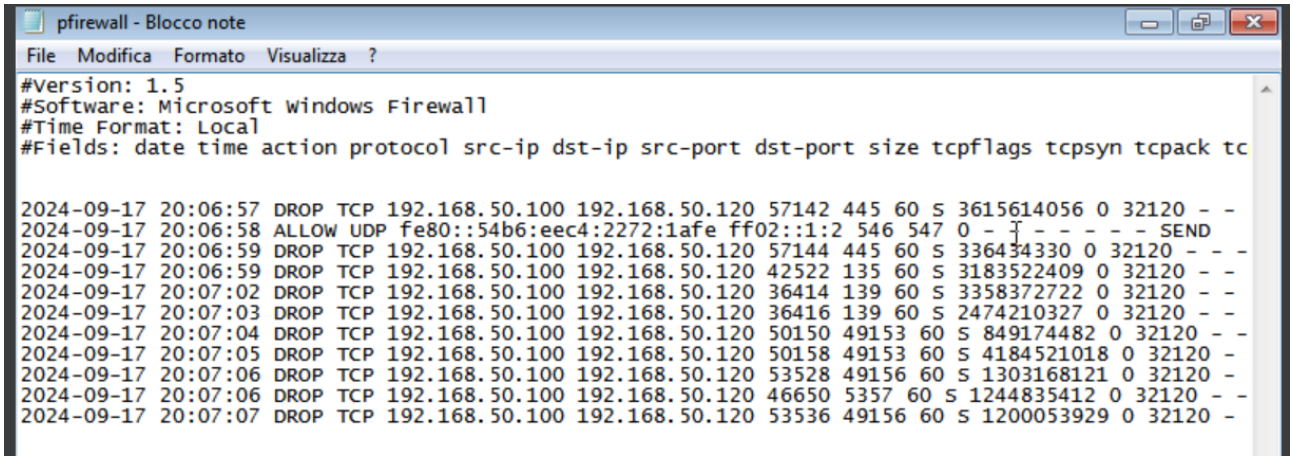
Scansione con il firewall windows disabilitato:

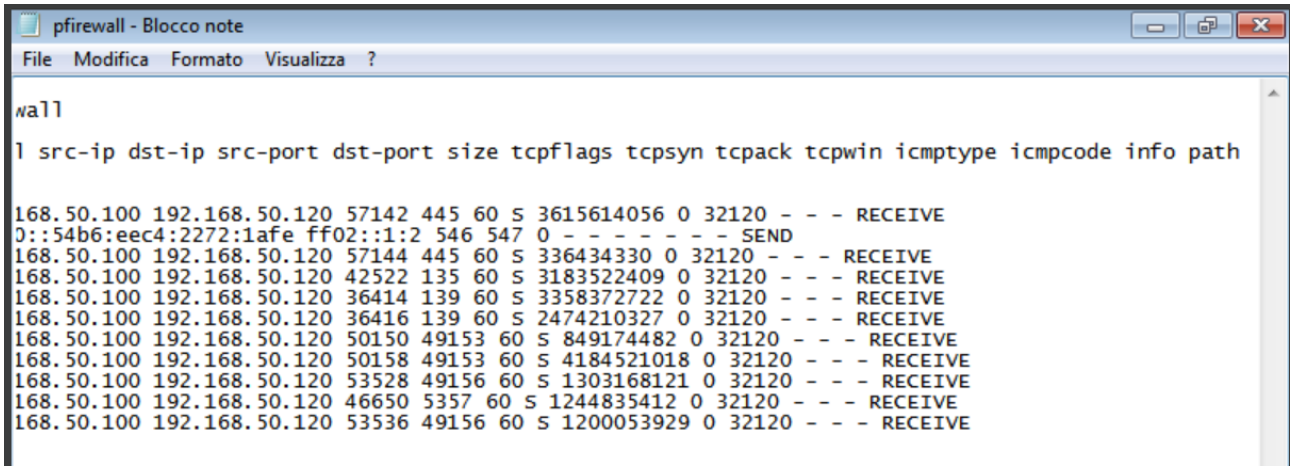


Scansione con il firewall abilitato:

Facoltativo

Log del firewall





Il log è strutturato in colonne con le seguenti informazioni:

- **src-ip**: Indirizzo IP sorgente.
- **dst-ip**: Indirizzo IP di destinazione.
- **src-port**: Porta sorgente.
- **dst-port**: Porta di destinazione.
- **size**: Dimensione del pacchetto.
- **tcpflags**: Flag TCP (S per SYN).
- **tcpsyn**: Numero di sequenza SYN.
- **tcpack**: Numero di sequenza ACK.
- **tcpwin**: Dimensione della finestra TCP.
- **icmptype** e **icmpcode**: Tipo e codice ICMP (non usati qui).
- **info**: Informazioni addizionali (RECEIVE/SEND).
- **path**: Percorso del pacchetto (non popolato in questo esempio).

Questi log forniscono dettagli su pacchetti TCP inviati e ricevuti, specificando la direzione, la sorgente, la destinazione e altri parametri relativi alla comunicazione di rete.

Cosa si riesce a trovare?

Monitorando questi log durante le operazioni di rete, puoi trovare informazioni come:

- **Conferme di connessione e disconnessione di rete:**
  - Eventi che registrano quando una connessione è stata stabilita o terminata, inclusi i dettagli su sorgente, destinazione, porte utilizzate, e protocolli.
- **Modifiche al firewall:**
  - Se vengono aggiunte, rimosse o modificate regole del firewall, queste azioni verranno registrate. È utile per tracciare se un'operazione ha cambiato il comportamento del firewall in modo non previsto.
- **Rilevamento di attacchi o tentativi di accesso non autorizzato:**
  - Se il firewall blocca delle connessioni non autorizzate o se ci sono tentativi di attacco, come scansioni di porte, questi eventi saranno visibili nel log del firewall o nel registro di sicurezza.
- **Trasmissioni o ricezioni di pacchetti inusuali:**
  - Eventi di sicurezza che potrebbero mostrare comportamenti sospetti, come pacchetti TCP non previsti o configurazioni IP inusuali.
- **Errori di connessione o servizi di rete falliti:**
  - Log relativi a problemi di connessione, come errori DHCP, DNS, o TCP/IP. Possono essere utili per risolvere problemi legati a configurazioni di rete o malfunzionamenti.
- **Autorizzazioni e tentativi di accesso:**
  - Se sono abilitati eventi di auditing legati all'accesso alla rete o alle modifiche di configurazione, potresti trovare tracce di chi ha effettuato certe operazioni, quando e da quale macchina.